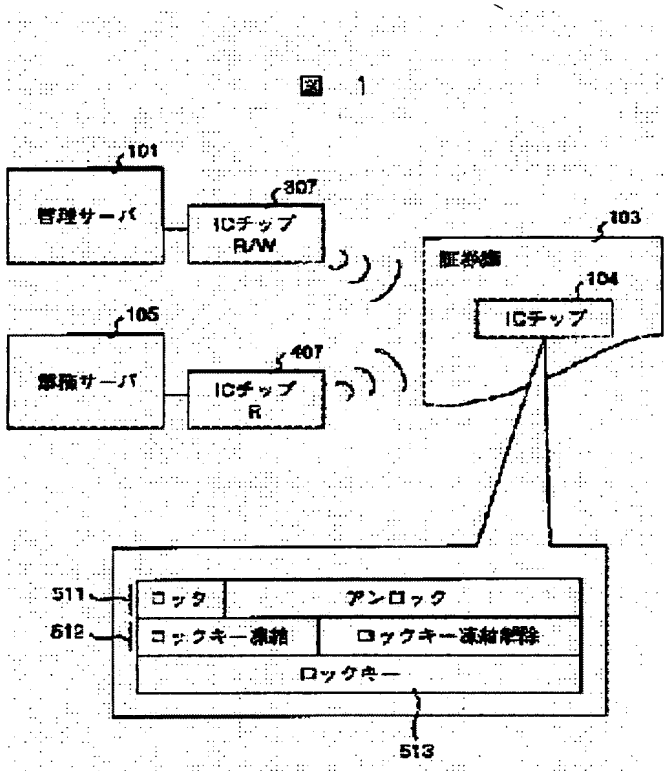
BILLS AS WELL AS VALUABLE PAPERS MOUNTING IC CHIP AND PREVENTING METHOD OF UNFAIR UTILIZATION OF THEM

Publication number: JP2001260580
Publication date: 2001-09-25
Inventor: TODA YUKITOSHI
Applicant: HITACHI LTD
Classification:
- international: ***B42D15/10; G06K17/00; G06K19/00; G06K19/07; G06Q10/00; G06Q40/00; G07D7/02;*** **B42D15/10; G06K17/00; G06K19/00; G06K19/07; G06Q10/00; G06Q40/00; G07D7/00;** (IPC1-7): B42D15/10; G06F17/60; G06K17/00; G06K19/00; G06K19/07; G07D7/02
- european:
Application number: JP20000077750 20000315
Priority number(s): JP20000077750 20000315

Abstract of **JP2001260580**

PROBLEM TO BE SOLVED: To provide valuable papers, capable of preventing unfair utilization by discriminating the cheating of the same and capable of reutilizing the papers when the papers can be taken back to a regular control source, and the preventing method of unfair utilization of them.
SOLUTION: A fine IC chip 104 is mounted on valuable papers 103, such as bills, stocks or the like, while the memory device of the IC chip 104 stores a lock information 511 and a lock key. The lock information 511 retains a condition of either one of lock/unlock. A business server 105 reads the condition of the lock information 511 through an IC chip reading device 407 and will not start a business process when the condition is not under the condition of unlock. A control server 101 communicates with the IC chip 104 through an IC chip reading and writing device 307 to certify that the lock key 513 is right and, thereafter, changes the condition of the lock information 511 if necessary.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－260580
（P2001－260580A）
(43)公開日　平成13年９月25日(2001.9.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｂ４２Ｄ　15/10	５３１	Ｂ４２Ｄ　15/10	５３１Ｂ	２Ｃ００５
	５２１		５２１	３Ｅ０４１
Ｇ０６Ｆ　17/60	２１４	Ｇ０６Ｆ　17/60	２１４	５Ｂ０３５
	５１０		５１０	５Ｂ０４９
	５１２		５１２	５Ｂ０５５

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願2000－77750(P2000－77750)

(22)出願日　平成12年３月15日(2000.3.15)

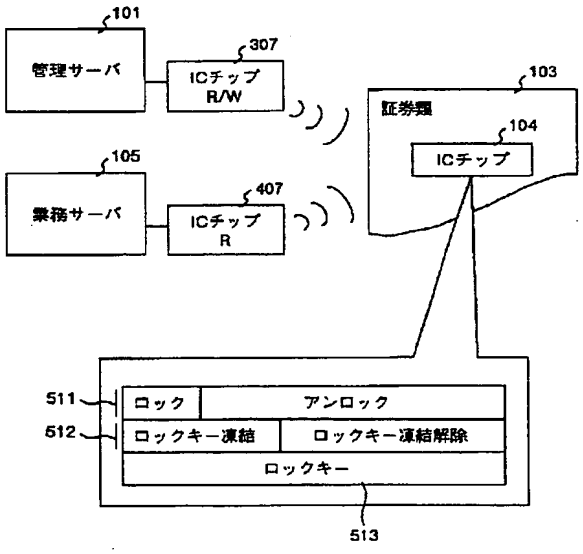
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　戸田　幸利
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所サービス事業部内
(74)代理人　100068504
弁理士　小川　勝男　（外１名）

最終頁に続く

(54)【発明の名称】　ＩＣチップを搭載する紙幣及び有価証券類並びにその不正利用防止方法

(57)【要約】
【課題】　証券類が搾取されたことを識別して不正利用を防ぐとともに、正規な管理元に取り戻せた場合には再利用が可能な証券類及びその不正利用防止方法を提供する。
【解決手段】　紙幣、株券など有価な証券類１０３に微細なＩＣチップ１０４が搭載されており、ＩＣチップ１０４の記憶装置はロック情報５１１及びロックキーを格納する。ロック情報５１１はロック／アンロックいずれかの状態を保持する。業務サーバ１０５は、ＩＣチップ読取装置４０７を介してロック情報５１１の状態を読み取り、それがアンロック状態でなければ業務処理を開始しない。管理サーバ１０１は、ＩＣチップ読取・書込装置３０７を介してＩＣチップ１０４と通信し、ロックキー５１３が正しいものと認証した後に、必要に応じてロック情報５１１の状態を変更する。

図　1



1

【特許請求の範囲】

【請求項１】非接触で読み書き可能なＩＣチップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記ＩＣチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能な情報と、外部からの要求に応答して前記情報を変更する前記ＩＣチップ内で実行可能なプログラムとを格納する記憶装置を有することを特徴とするＩＣチップを搭載する有価証券類。

【請求項２】非接触で読み書き可能なＩＣチップを搭載する紙幣、商品券、株券、債券など有価の証券類の不正利用防止方法であって、前記ＩＣチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック／アンロック情報と、外部からの要求に応答して前記ロック／アンロック情報の参照と更新を行う前記ＩＣチップ内で実行可能なプログラムとを格納する記憶装置を有し、前記証券類の利用を禁止するように外部の計算機によって前記ＩＣチップに前記ロック／アンロック情報をロック状態に設定するように指令し、前記証券類を利用可能とするように外部の計算機によって前記ＩＣチップに前記ロック／アンロック情報をアンロック状態に設定するように指令し、外部の計算機によって前記ＩＣチップ上の前記ロック／アンロック情報を参照し、前記ロック／アンロック情報がアンロック状態の場合に業務処理を開始することを特徴とするＩＣチップを搭載する有価証券類の不正利用防止方法。

【請求項３】前記ロック／アンロック情報を更新する前記外部の計算機は、その記憶装置に第１のキー情報を保存し、前記ＩＣチップはその記憶装置に第１のキー情報と対になる第２のキー情報を保存し、前記ロック／アンロック情報を更新する前記外部の計算機と前記ＩＣチップとの間で第１のキー情報と第２のキー情報とが所定の対応関係をもつことを認証したとき、前記ＩＣチップによって前記ロック／アンロック情報の更新を行うことを特徴とする請求項２記載のＩＣチップを搭載する有価証券類の不正利用防止方法。

【請求項４】非接触で読み書き可能なＩＣチップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記ＩＣチップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック／アンロック情報と、外部からの要求に応答して前記ロック／アンロック情報の参照と更新を行う前記ＩＣチップ内で実行可能なプログラムとを格納する記憶装置を有するところの有価証券類と、前記ＩＣチップに対して前記ロック／アンロック情報を更新するよう指令する管理用計算機と、前記ＩＣチップに要求して前記ロック／アンロック情報を参照し、前記ロック／アンロック情報がアンロック状態の場合に業務処理を開始する業務処理用計算機とを有することを特徴とするＩＣチップを搭載する有価証券類の不正利用防止システム。

【請求項５】前記ロック／アンロック情報を更新する前記管理用計算機は、その記憶装置に第１のキー情報を保存し、前記ＩＣチップはその記憶装置に第１のキー情報と対になる第２のキー情報を保存し、前記ロック／アンロック情報を更新する前記管理用計算機と前記ＩＣチップとの間で第１のキー情報と第２のキー情報とが所定の対応関係をもつことを認証したとき、前記ＩＣチップが前記ロック／アンロック情報の更新を行うことを特徴とする請求項４記載のＩＣチップを搭載する有価証券類の不正利用防止システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、金融／サービス／運送業などの取扱い対象となる証券類及びその不正利用防止方法に係わり、特に紙幣、商品券、株券、債券、手形、小切手など何らかの価値を持つ有価証券類（以下、単に証券類と呼ぶ）を保管、運搬する際に盗難等で不正に取得した証券類を使用不可の状態にしたり、正規に入手した証券類の有効性を証明する不正利用防止システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】従来、取引の支払いをしたり、商品の引換えをしたり、株式会社に出資したり、第三者から事業資金を得たり、代金の支払いの約束をしたり、金銭の支払いの約束をしたりと、様々な価値をもつ権利を表す証券類が世の中に流通している。

【０００３】これらの証券類を一時的に保管したり、運搬したりする場合には、物理的な鍵のかかる金庫やトランクなどに鍵を掛けたり、盗難を防ぐために警備員を配置したりするが、証券類には特に何らかの加工を加えることはせず、現状はそのまま利用可能な状態にある。

【０００４】なお、近年は街頭に置かれた無人のＡＴＭ／ＣＤ端末を、パワーシャベルなどといった重機を使って破壊し、保管してある現金を搾取したりすることがあるので、ＡＴＭ／ＣＤ端末に破壊などの不正行為を働いた場合に、紙幣にインクを吹き付けたりして盗難にあった事実を記したりする技術がある。

【０００５】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。すなわち一旦盗難にあった証券類は、正規に利用されるものと区別のつかない状態にあって不正に利用されたり、インクなどの目印が付いてしまい、正当な所有者が取り戻すことができても再利用できないという問題がある。またインクが搾取される証券類の全数に確実につかない可能性もある。

【０００６】本発明の目的は上記問題を解決し、盗難された証券類の不正利用を防止したり、正規の管理元に取り戻した場合に再利用することが可能な証券類及びその不正利用防止方法を提供することにある。

【０００７】

【課題を解決するための手段】本発明は、保管または輸

送される証券類について、証券類に搭載したＩＣチップの情報を読んで、不正に搾取されたものとして利用してはならないか、あるいは正規に譲渡されたものとして利用して良いものかどうかを識別可能にするものである。

【０００８】本発明において、証券類の利用の可否を識別するには、証券類に搭載したＩＣチップに利用可否の識別情報を登録することによって行う。近年になってサイズが数ミリ（２～３㎜）角の非接触通信式のＩＣチップ（ＲＦＩＤ）の開発が新聞等で発表されてきている。こういった微細なＩＣチップ製造技術がさらに進めば、紙幣や有価証券などに装着できるようなＩＣチップが登場する。本発明では、こういった紙などの薄い媒体に微細なＩＣチップを本発明でいう証券類の一枚ずつに搭載し、当該証券類各々の有効性の情報をもたせ、それらの情報を読み込んで識別することを可能にするものである。

【０００９】証券類に搭載するＩＣチップへの読み書きは、当該証券類を保管／運搬の管理をする法人または事業所の管理単位に可能であり、ＩＣチップへの情報の書き込みに関するセキュリティも管理する。よって正規の管理元が保管または運搬する証券類を他者が搾取したとき、当該証券類に搭載するＩＣチップの情報が利用不可の状態であることを示すようにしておき、証券類の利用時にこの情報を読み出すことによって、当該証券類が不正に搾取されたものであることを識別でき、これらをこの状態で利用することを拒否することによって、不正利用を防止することが可能になる。証券類に搭載するＩＣチップの情報の読み取りは、証券類を業務処理に使用する際にＩＣチップ読取装置で読み取ることができるようにしておく。

【００１０】一方、証券類に搭載したＩＣチップへの情報の書き込みは、セキュリティのための制御情報（暗証番号、暗号鍵など）により、このような制御情報を保持する管理用計算機のみが行えるようにし、制御情報を知らない第三者がＩＣチップの情報を書き換えることはできないようにする。

【００１１】またある管理元が管理する証券類を別の管理元に正規に移管する場合には、新しい管理元が譲渡対象となる証券類に搭載するＩＣチップの情報を書き換えるために必要な独自の制御情報に変更できるように、古い管理元が設定していた制御情報を用いて制御情報の書き換え制限を解除することにより、新しい管理元が管理する制御情報に変更することができる。こうして新たな管理元は、自分の管理下のセキュリティ制御情報を用いて証券類に搭載するＩＣチップの情報を必要に応じて書き換えることができるようになる。

【００１２】よって一旦不正に搾取された証券類でも、元のＩＣチップの情報を書き換えできる正当なセキュリティ制御情報をもつ管理元に戻せれば、利用不可状態となっていた証券類のＩＣチップの情報を利用可能な状態に戻すことができ、問題なく再利用することができるようになる。

【００１３】以上のように本発明の証券類及びその不正利用防止方法によれば、非接触の通信によりＩＣチップを搭載した管理単位全数について確実に証券類の利用可否の情報を読み書きできるので、搾取された証券類を識別でき、その不正利用を防ぐことができ、さらに正規の所有者の手に戻れば再度利用可能な状態に戻すことも可能である。

【００１４】

【発明の実施の形態】以下に証券類の不正利用防止を可能とする実施形態について図面を用いて説明する。

【００１５】図１は、本実施形態の概略構成を示す図である。証券類１０３には微細なＩＣチップ１０４が装着されている。ＩＣチップ１０４は、証券類１０３を構成する２枚の紙の間にすき込むか、あるいはＩＣチップ１０４を封入したシールを証券類１０３に接着するなどの方法によって証券類１０３に装着されている。いずれにしてもＩＣチップ１０４は、証券類１０３を使用不可能にするほど破損することなく、そのＩＣチップ１０４を証券類１０３から引き離すことができないような方法で証券類１０３に装着されている。ＩＣチップ１０４内の記憶装置にはロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３を記録する。ロック情報５１１は、ロック状態とアンロック状態のいずれかの状態をもつ。ロック状態は業務処理のために証券類１０３を利用できない状態であり、アンロック状態は業務処理のために証券類１０３を利用できる状態である。ロックキー５１３は、ロック情報５１１、ロックキー凍結情報５１２およびロックキー５１３自体を変更するために必要な鍵（パスワード、暗号鍵など）となるビット列である。ロックキー凍結情報５１２は、ロックキー凍結状態とロックキー凍結解除状態のいずれかの状態をもつ。ロックキー凍結状態はロックキー５１３を凍結し更新できない状態であり、ロックキー凍結解除状態はロックキー５１３を更新できる状態である。

【００１６】管理サーバ１０１は、ロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３を更新する権限をもち、ロックキー５１３を管理する計算機であり、ＩＣチップ読取・書込装置３０７を接続する。管理サーバ１０１は、ＩＣチップ読取・書込装置３０７を介して証券類１０３に搭載されたＩＣチップ１０４上の情報を非接触で読み取り、ロック情報５１１の変更、ロックキー凍結情報５１２の変更及びロックキー５１３の更新を行う。

【００１７】業務サーバ１０５は、証券類１０３に関する業務処理を行う計算機であり、ＩＣチップ読取装置４０７を接続する。業務サーバ１０５は、ＩＣチップ読取装置４０７を介して証券類１０３のＩＣチップ１０４上のロック情報５１１にアクセスし、ロック情報５１１が

アンロック状態であれば証券類１０３を取り扱う業務処理を行い、ロック状態であれば業務処理を行わない。

【００１８】図２は、ＩＣチップ１０４の装着された証券類１０３を利用する手順の例を説明する図である。ＩＣチップ１０４の装着された証券類１０３は、証券類１０３の製造過程から入ってきた証券類１０３であり最初に利用されるものであるか、または他の管理サーバによって管理されていたものであって最初に当該管理サーバ１０１の管理下に入るものとし、ロック情報５１１がロック状態、ロックキー凍結情報５１２がロックキー凍結の状態にあるものとする。

【００１９】図２（ａ）は、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロックキー凍結情報５１２をロックキー凍結解除し、ロックキー５１３を自分の管理するロックキーに更新するステップである。図２（ｂ）は、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロック情報５１１をロック状態にし、ロックキー凍結情報５１２をロックキー凍結の状態に変更するステップである。図２（ｃ）は、この状態の証券類１０３を保管または運搬するステップを示す。この状態の証券類１０３を業務処理に利用することはできない。また他の管理サーバによって不当にロックキー５１３を自分の管理下のロックキーに更新することはできない。

【００２０】図２（ｄ）は、この証券類１０３を業務処理に利用するために、管理サーバ１０１が証券類１０３上のＩＣチップ１０４についてロック情報５１１をアンロックの状態に変更するステップである。図２（ｅ）では、業務サーバ１０５が証券類１０３上のＩＣチップ１０４のロック情報５１１にアクセスして利用の可否をチェックする。ロック情報５１１がアンロック状態であればこの証券類１０３に関する業務処理を開始し、ロック情報５１１がロック状態であればこの証券類１０３についての業務処理を行わない。従って保管または運搬中に盗難等に会った証券類１０３は業務処理されない。

【００２１】上記の証券類１０３がある管理サーバの管理下から別の管理サーバの管理下に移るとは、例えば証券類１０３がある金融機関から別の金融機関に譲渡されたり、事業所間で譲渡される場合を想定している。従ってセキュリティの問題が生じないのであれば、ＩＣチップ１０４のロック情報５１１がアンロック、ロックキー凍結情報５１２がロックキー凍結解除の状態で証券類１０３を事業所間で譲渡しても構わない。

【００２２】図３は、管理サーバ１０１の概略構成を示す図である。図３に示すように管理サーバ１０１は、ＣＰＵ３０１と、メモリ３０２と、磁気ディスク装置３０３と、キーボード装置３０４と、ディスプレイ装置３０５と、ＣＤ－ＲＯＭ装置３０６と、ＩＣチップ読取・書込装置３０７を有している。磁気ディスク装置３０３はロックキー管理テーブル３０８を格納している。管理サーバ１０１の全体が携帯情報処理装置であってもよい。

【００２３】ＣＰＵ３０１は、管理サーバ１０１全体の動作を制御する装置である。メモリ３０２は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置３０３は、各種処理プログラムやデータを格納しておく記憶装置である。キーボード装置３０４は、データ入力のための装置であり、ディスプレイ装置３０５は各種データの表示を行う装置である。ＣＤ－ＲＯＭ装置３０６は、各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。ＩＣチップ読取・書込装置３０７は、証券類１０３に搭載するＩＣチップ１０４との間で非接触で情報の読み書きをする装置である。

【００２４】ロックキー管理テーブル３０８は、当該管理サーバ１０１が管理するロックキーを格納するテーブルである。

【００２５】ロック／ロックキー処理部３１０は、メモリ３０２に格納され、図２に示すように証券類１０３のＩＣチップ１０４に記録されたロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３の管理に係わる処理を行うプログラムであり、ＣＰＵ３０１によって実行される。

【００２６】ＣＤ－ＲＯＭ等の記録媒体に記録されたロック／ロックキー処理部３１０を磁気ディスク装置３０３等に格納した後、メモリ３０２にロードして実行するものとする。なおこのプログラムを記録する記録媒体としてＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００２７】図４は、業務サーバ１０５の概略構成を示す図である。図４に示すように業務サーバ１０５は、ＣＰＵ４０１と、メモリ４０２と、磁気ディスク装置４０３と、キーボード装置４０４と、ディスプレイ装置４０５と、ＣＤ－ＲＯＭ装置４０６と、ＩＣチップ読取装置４０７とを有している。

【００２８】ＣＰＵ４０１は、業務サーバ１０５全体の動作を制御する装置である。メモリ４０２は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置４０３は、各種処理プログラムやデータを格納しておく記憶装置である。ＩＣチップ読取装置４０７は、証券類１０３に搭載するＩＣチップ１０４から非接触でロック情報５１１を読み取る装置である。

【００２９】メモリ４０２は、ロック判定処理部４１０及び業務処理部４１１を格納する。ロック判定処理部４１０は、証券類１０３に搭載するＩＣチップ１０４のロック情報５１１を読み込み、当該証券類１０３の利用の可否を判定する処理を行うプログラムである。業務処理部４１１は、利用可能と判定した証券類１０３に関する業務アプリケーションの処理を行う処理部である。

【００３０】ＣＤ－ＲＯＭ等の記録媒体に記録されたロック判定処理部４１０を含むプログラムを磁気ディスク装置４０３等に格納した後、メモリにロードして実行す

るものとする。なおこのプログラムを記録する記録媒体としてＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００３１】図５は、証券類１０３に搭載されるＩＣチップ１０４の内部構成を示す図である。ＩＣチップ１０４は、微細な半導体チップであり、図５に示すように通信アンテナ５０１、電磁誘導起電装置５０２、電力蓄積装置５０３、制御装置５０４及び記憶装置５０５を有している。

【００３２】通信アンテナ５０１は、ＩＣチップ１０４とＩＣチップ読取・書込装置３０７又はＩＣチップ読取装置４０７との間で情報を送受信したり、ＩＣチップ１０４を駆動する電源となる電力供給のための電磁波をＩＣチップ読取・書込装置３０７又はＩＣチップ読取装置４０７から受けたりする装置である。電磁誘導起電装置５０２は、通信アンテナ５０１で受けた電磁波を電磁誘導により電力に変換する装置である。電力蓄積装置５０３は、電磁誘導起電装置５０２で起電した電力を蓄積して、ＩＣチップ１０４を駆動するための電源とする装置である。

【００３３】制御装置５０４は、マイクロプロセッサを含み、ＩＣチップ１０４全体の動作を制御する装置である。記憶装置５０５は、ロック情報５１１、ロックキー凍結情報５１２及びロックキー５１３の管理情報と、暗号復号プログラム５２１、ロックキー正否判定プログラム５２２、ロック状態参照更新プログラム５２３、ロックキー更新プログラム５２４など各種プログラムを格納する。

【００３４】ロック情報５１１は、ロック／アンロックの状態を示す１ビットの情報を格納する。ロックキー凍結情報５１２は、ロックキー凍結／ロックキー凍結解除を示す１ビットの情報を格納する。ロックキー５１３は当該ＩＣチップ１０４に付与される鍵として管理される情報である。

【００３５】図６は、ＩＣチップ１０４に記録されるロック情報５１１及びロックキー凍結情報５１２の状態遷移について説明する図である。ロック情報５１１及びロックキー凍結情報５１２の状態は、ロックかつロックキー凍結の状態６０１と、アンロックかつロックキー凍結の状態６０２と、アンロックかつロックキー凍結解除の状態６０３の３つがある。

【００３６】状態６０１は、当該証券類１０３を利用不可能で、かつロックキー５１３を更新することができない状態である。正しいロックキーを用いることによって状態６０１から状態６０２に遷移することができる。

【００３７】状態６０２は、当該証券類１０３を利用することが可能で、かつロックキー５１３を更新することができない状態である。正しいロックキーを用いることによって状態６０２から状態６０３に遷移することができる。また正しいロックキーを用いることによって状態６０２から状態６０１に遷移することができる。

【００３８】状態６０３は、当該証券類１０３を利用することが可能で、かつロックキー５１３を更新することができる状態である。正しいロックキーを用いることによって状態６０３から状態６０２に遷移することができる。

【００３９】図７Ａ及び図７Ｂは、管理サーバ１０１のロック／ロックキー処理部３１０の処理の流れを示すフローチャートである。ロック／ロックキー処理部３１０は、対象とする証券類１０３についてキーボード等から入力された要求を受け取る（ステップ７０１）。要求は次に示す４種類ある。（１）当該証券類１０３に搭載されたＩＣチップ１０４のロック情報５１１をアンロック状態からロック状態に変更する。（２）ロック情報５１１をロック状態からアンロック状態に変更する。この要求ではロックキー凍結情報５１２をロックキー凍結状態にするか、ロックキー凍結解除の状態にするかの指定が必要である。（３）ロック情報５１１をアンロック状態、ロックキー凍結情報５１２をロックキー凍結解除状態にした後にロックキー５１３を更新する。（４）ロックキー５１３を更新した後にロック情報５１１をロック状態、ロックキー凍結情報５１２をロックキー凍結状態にする。

【００４０】次にロック／ロックキー処理部３１０は、ロックキー５１３が正しいか否か、例えば古い管理元から通知を受けたロックキーであってキーボード３０４などから入力されたロックキー又はロックキー管理テーブル３０８に登録されているロックキーとＩＣチップ１０４上のロックキー５１３とが一致するか否か判定する（ステップ７０２）。ここではまだロックキー５１３が更新されていないため、ロックキー更新前のロックキーについて照合することになり、そのロックキーは当該管理サーバ１０１が管理するロックキー又は他の管理事業所から通知を受けたロックキーのいずれかである。ロックキー５１３が正しくなければ（ステップ７０２，誤り）、処理終了とする。

【００４１】ロックキー５１３が正しければ、当該ＩＣチップ１０４上のロック情報５１１をアンロック状態に変更するアンロック処理を行う（ステップ７０３）。次にロックキーの更新が要求されていなければ（ステップ７０４，しない）、ステップ７０９へ行く。ロックキーの更新が要求されている場合には、ロックキー５１３が正しいか否か判定する（ステップ７０５）。ここではステップ７０２のチェックが繰り返されることになり、ロックキー５１３が正しいと判定される。次にロックキー凍結情報５１２を読み取り、ロックキー凍結状態であれば（ステップ７０６，凍結）、これをロックキー凍結解除の状態にする（ステップ７０７）。次にロックキー管理テーブル３０８を参照してＩＣチップ１０４上のロックキー５１３を管理サーバ１０１の管理下にある新しいロックキーに更新する（ステップ７０８）。

【００４２】次に図７Ｂに移り、ロック／ロックキー処理部３１０は、ロックキーを凍結するか否か判定する（ステップ７０９）。要求（１）、（４）及び（２）でロックキー凍結の指定がされた場合にはロックキーの凍結が必要である。ロックキー凍結しない場合にはステップ７１２へ行く。次にロックキー５１３が正しいか否か判定する（ステップ７１０）。ステップ７０８のロックキー更新をした場合には、ロックキー管理テーブル３０８上のロックキーと更新後のロックキー５１３との一致が判定されるわけであり、当然ロックキー５１３が正しいと判定される。ステップ７０８のロックキー更新をしていない場合には、ステップ７０２のチェックが繰り返されることになり、ロックキー５１３が正しいと判定される。ロックキーが正しければ（ステップ７１０，正しい）、ロックキー凍結情報５１２をロックキー凍結状態にする（ステップ７１１）。

【００４３】次にロック／ロックキー処理部３１０は、ロック情報５１１をロック状態にするか否か判定する（ステップ７１２）。要求（１）および（４）については、ロック情報５１１をロック状態にする必要がある。ロックする場合（ステップ７１２，する）には、再びロックキー５１３が正しいか否か判定する（ステップ７１３）。要求（１）及び（４）の場合にはステップ７０２及びステップ７１０のチェックが繰り返されることになり、ロックキー５１３が正しいと判定される。ロックキーが正しければ（ステップ７１３，正しい）、ロックキー凍結情報５１２が凍結の状態であり（ステップ７１４，凍結）、ロック情報５１１がアンロック状態の場合に（ステップ７１５，アンロック）、ロック情報５１１をロック状態に変更するロック処理を行う（ステップ７１６）。

【００４４】ステップ７１０でロックキーの誤りがある場合、ステップ７１２でロックしない場合、ステップ７１３でロックキーの誤りがある場合、ステップ７１４でステップ７０９の判定と矛盾するロックキー凍結情報５１２がロックキー凍結解除状態の場合、およびステップ７１５でロック情報５１１がロック状態の場合には直ちに処理終了とする。

【００４５】上記実施形態では、ロックキー５１３が正しいか否かのチェックは、別の管理下にあったロックキー又はロックキー管理テーブル３０８上のロックキーとＩＣチップ１０４上のロックキー５１３とが一致するか否かの判定によっていたが、管理サーバ１０１からＩＣチップ読取・書込装置３０７を介してＩＣチップ１０４へ平文のままのロックキーを伝送したり、ＩＣチップ１０４から管理サーバ１０１へ平文のままのロックキーを伝送すると、セキュリティが破られる危険性が高くなる。たとえばＩＣチップ読取・書込装置３０７から送出される電磁波を盗聴すれば管理サーバ１０１とＩＣチップ１０４との間に伝送されるロックキーを知り得ることになる。このような危険を避けるために、直接ロックキーを伝送せずにロックキーを暗号鍵とし、ロックキーによって暗号化した数値を伝送するのが望ましい。たとえばロックキー管理テーブル３０８に登録するロックキーを公開鍵とし、ロック／ロックキー処理部３１０が乱数を発生させ、発生した乱数をこの公開鍵で暗号化して暗号化した乱数と元の乱数とをＩＣチップ１０４へ伝送する。ＩＣチップ１０４のロックキー正否判定プログラム５２２は、ロックキー正否判定のコマンドを受けたとき、暗号復号プログラム５２１が秘密鍵として保存するロックキー５１３によって暗号化された乱数を復号し、ロックキー正否判定プログラム５２２が復号された乱数と元の乱数とを比較してロックキーの正否を判定し、その結果（正または否）を管理サーバ１０１のロック／ロックキー処理部３１０に通知することが可能である。この場合には別の管理下にあったロックキー又はロックキー管理テーブル３０８上のロックキーとＩＣチップ１０４上のロックキー５１３とは公開鍵ペアの対応関係をもち、一般に同一値とはならない。従って一般にはいずれかの管理下にあるロックキーとＩＣチップ１０４上のロックキー５１３とは同一値である必要はなく、所定の対応関係をもった数値であればよい。

【００４６】ＩＣチップ１０４上のロック状態参照更新プログラム５２３は、管理サーバ１０１又は業務サーバ１０５からそのロック情報５１１の参照を要求するコマンドを受けたとき、ロックキーの正否が判定済であるなしに係わらずロック情報５１１の内容を要求元に送信する。しかしロック情報５１１の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム５２２によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。またロック状態参照更新プログラム５２３は、ロックキー凍結情報５１２の参照又は更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム５２２によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。

【００４７】同様にＩＣチップ１０４上のロックキー更新プログラム５２４は、ロックキー５１３の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム５２２によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。ロックキーとして公開鍵ペアを使用する場合には、ロック／ロックキー処理部３１０は、ＩＣチップ１０４へロックキー５１３の更新要求コマンドを伝送して応答を得た後に、更新後のロックキー（秘密鍵）を古いロックキー（公開鍵）で暗号化してＩＣチップ１０４へ送信する。ロックキー更新プログラム５２４は、暗号復号プログラム５２１を介して受け取った暗号化情報をロックキー５１３に格納される古いロックキー（秘密鍵）で復号し、ロックキー５１３を復号された新しいロックキー（秘密鍵）に置き換える。ロックキーとして公開鍵ペアの代わりに共通鍵を

使用する場合には、同様にロック／ロックキー処理部３１０が新しいロックキー（共通鍵）を古いロックキー（共通鍵）で暗号化してＩＣチップ１０４へ送信し、ロックキー更新プログラム５２４が受け取った暗号化情報を古いロックキー（共通鍵）で復号し、ロックキー５１３を得られたロックキーに置き換える。

【００４８】ロックキー正否判定プログラム５２２は、記憶装置５０５上にロックキー正否判定フラグをもち、ロックキーの正否判定の結果（正または否）を保存する。そしてステップ７０３の処理（アンロック処理）、ステップ７０８の処理（ロックキーの更新）、ステップ７１１の処理（ロックキーの凍結処理）及びステップ７１６の処理（ロック処理）の各々の処理終了時にこのロックキー正否判定フラグを初期状態（否）にリセットする。このような構成によって要求（１）～（４）のいずれの場合にも処理終了時にこのフラグが否の状態にリセットされている。

【００４９】なお上記実施形態ではＩＣチップ１０４にロックキー凍結情報５１２を設け、ロックキー凍結情報５１２がロックキー凍結解除状態のときのみロックキー５１３を更新可能としたが、ロックキー凍結情報５１２を設けず、ロック情報５１１の状態に係わらずロックキーが正しい場合には常にロックキー５１３更新可能とするように縮退した形でも本発明を実施できる。その場合には要求は（１）及び（２）と（３）又は（４）の３種類となり、ステップ７０６，７０７，７０９，７１０，７１１及び７１４の処理は除外される。

【００５０】またＩＣチップ１０４の記憶装置５０５に当該ＩＣチップ１０４の製造番号のような識別番号（ＩＤ）をもたせ、ロックキー管理テーブル３０８にはこのＩＤとロックキーとの対応テーブルを設け、ＩＤとロックキーとの対でＩＣチップ１０４を搭載した証券類１０３を管理してもよい。またＩＣチップ１０４を単に保管又は輸送中の盗難防止という目的で使用するのであれば、管理サーバ１０１が管理下におくすべての証券類１０３のＩＣチップ１０４に同一のロックキーを付与して管理することも可能である。盗難等から取り戻されたロック状態におかれたＩＣチップ１０４を搭載する証券類１０３は、当該管理サーバ１０１のみがアンロックの状態にできる。

【００５１】あるいは上記実施形態についての変形例として、ＩＣチップ１０４のロック情報５１１に対し、あらかじめ特別に規定したロックキー５１３の無効を示す値を設定すると、永久にアンロック状態に戻れない仕組みにしておけば、例えば使用後の商品券を再使用できないように裁断（廃棄）処理するなどと同様に、本発明の証券類に対して、電子的な廃棄処理を施すことができる。

【００５２】以上述べたように、本発明の実施に当っては色々の変形ができるので、セキュリティの必要程度とＩＣチップ１０４のコストとの兼ね合いで、ＩＣチップ１０４のハードウェア及びＩＣチップ１０４に格納しＩＣチップ１０４が実行するプログラムの機能を決めればよい。

【００５３】上記のように本実施形態では、当該証券類に対する業務処理の実行の可否を業務サーバが管理サーバにオンラインネットワークなどで問い合わせることなく、当該証券類に搭載したＩＣチップの情報から判定し、正当に業務処理を行ったり、不正な利用を防止したりすることが可能である。また本発明の方法を適用し、一旦搾取された利用不可能な証券類を正当な管理サーバの管理下に取り戻せた場合は、その再利用を可能とすることができる。

【００５４】以上説明したように本実施形態によれば、証券類に搭載したＩＣチップの情報を用いて当該証券類の利用の可否を判定できるので、不正に搾取された証券類かどうかをその場で識別して不正利用を未然に防ぐことが可能である。

【００５５】

【発明の効果】本発明によれば、証券類に搭載したＩＣチップの情報を用いて不正に搾取された証券類を識別できるので、不正利用を防止することができ正当な管理元に戻せた場合に再利用可能な状態に戻すことが可能である。

【図面の簡単な説明】

【図１】実施形態の概略構成を示す図である。

【図２】実施形態のＩＣチップを搭載する証券類の利用手順を説明する図である。

【図３】実施形態の管理サーバ１０１の概略構成を示す図である。

【図４】実施形態の業務サーバ１０５の概略構成を示す図である。

【図５】実施形態の証券類１０３に搭載されるＩＣチップ１０４の内部構成を示す図である。

【図６】実施形態のロック情報５１１及びロックキー凍結情報５１２の状態遷移を示す図である。

【図７Ａ】実施形態の管理サーバ１０１のロック／ロックキー処理部３１０の処理手順を示すフローチャートである。

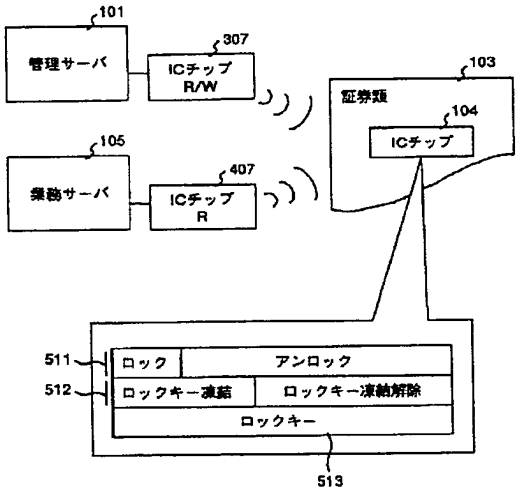
【図７Ｂ】実施形態の管理サーバ１０１のロック／ロックキー処理部３１０の処理手順を示すフローチャート（続き）である。

【符号の説明】

１０１…管理サーバ、１０３…証券類、１０４…ＩＣチップ、１０５…業務サーバ、３０８…ロックキー管理テーブル、３１０…ロック／ロックキー処理部、５１１…ロック情報、５１２…ロックキー凍結情報、５１３…ロックキー

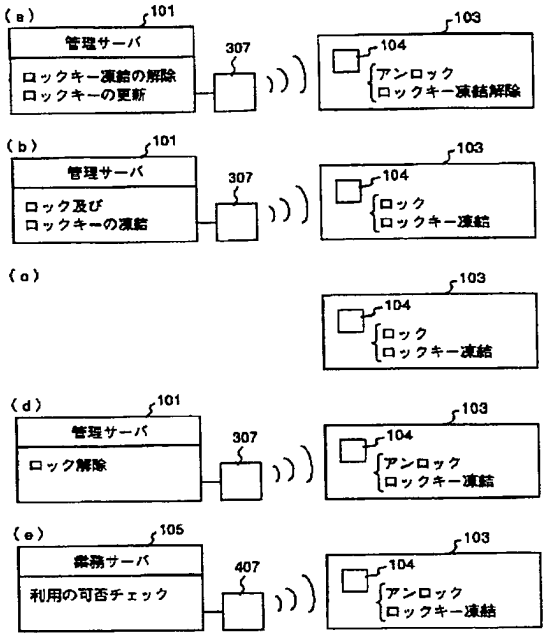
【図１】

図　1



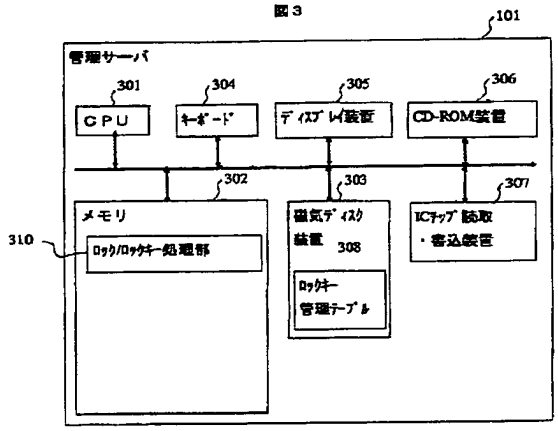
【図２】

図　2



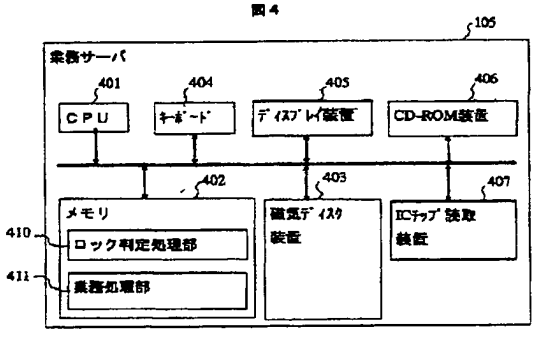
【図３】

図３



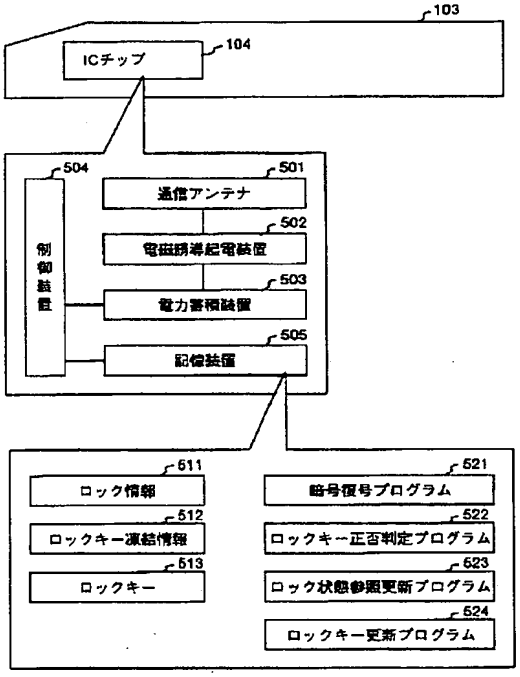
【図４】

図４



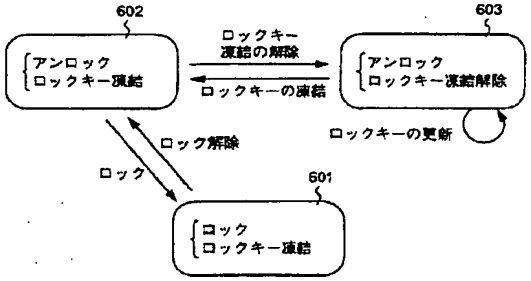
【図５】

図 5



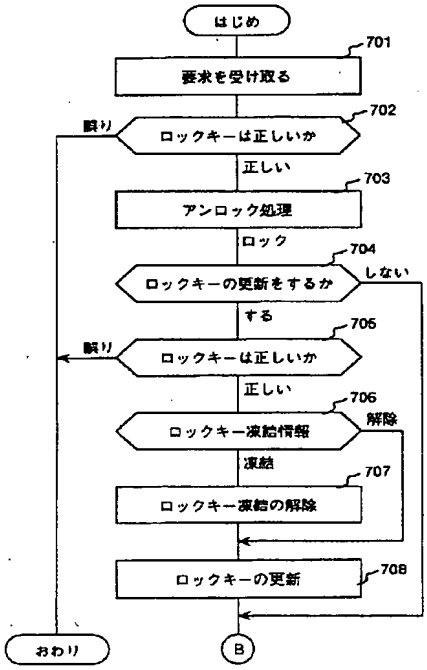
【図６】

図 6



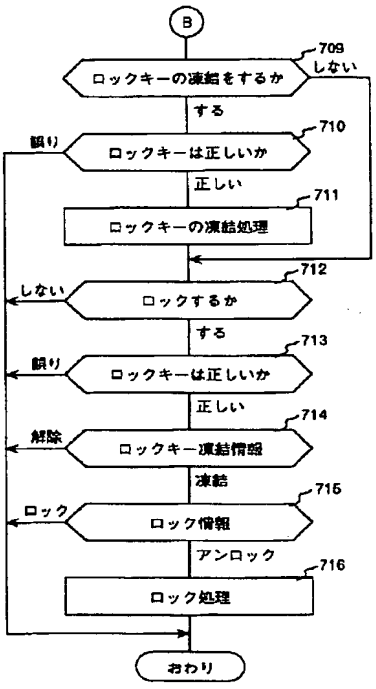
【図７Ａ】

図 7A



【図７Ｂ】

図 7B



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード（参考）
Ｇ０６Ｋ 17/00		Ｇ０６Ｋ 17/00		Ｌ ５Ｂ０５８
				Ｆ
19/07		Ｇ０７Ｄ 7/02		
19/00		Ｇ０６Ｋ 19/00		Ｈ
Ｇ０７Ｄ 7/02				Ｑ

Ｆターム(参考) 2C005 HA01 HA02 HB10 JA09 JB40
LB20 LB32 MA01 MA03 MA40
MB10 NA09 PA02 QA05 SA06
SA07 SA08
3E041 AA01 AA02 AA03 BA20 BB07
DB01
5B035 AA13 BA01 BB09 CA23
5B049 AA05 BB47 CC39 DD01 DD04
DD05 EE03 EE23 EE25 EE28
FF03 FF04 FF08 FF09 GG03
GG06 GG10
5B055 CC10 CC13 EE02 EE13 EE17
EE21 EE27 HA12 JJ05 KK05
KK09 KK18 PA02 PA34
5B058 CA15 KA01 KA31 KA35